

The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should not be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

Vulnerabilities

- Windows Operating Systems
 - [@Mail Webmail Arbitrary Code Execution](#)
 - [Aquifer CMS Cross-Site Scripting\(Updated\)](#)
 - [Community Server Cross-Site Scripting](#)
 - [CA Unicenter TNG Denial of Service](#)
 - [Hosting Controller SQL Injection](#)
 - [eXchange POP3 Arbitrary Code Execution](#)
 - [Lexmark Printer Sharing Service Arbitrary Code Execution](#)
 - [ASPSurvey SQL Injection](#)
 - [MailEnable Enterprise Edition Webmail Denial of Service](#)
 - [Microsoft HTML Help Workshop Arbitrary Code Execution](#)
 - [Microsoft Internet Explorer Denial of Service](#)
 - [Internet Explorer Arbitrary Code Execution](#)
 - [Microsoft Windows Privilege Elevation](#)
 - [Winamp Denial of Service](#)
 - [The Bat! Spoofing](#)
 - [Symantec Sygate Management Server SQL Injection or Unauthorized Access](#)
 - [Trend Micro ServerProtect Arbitrary Code Execution](#)
 - [WiredRed E/POP Web Conferencing HTML Injection](#)
- Unix/ Linux Operating Systems
 - [BlueZ Project hcidump Bluetooth L2CAP Remote Denial of Service](#)
 - [Bogofilter Multiple Remote Buffer Overflows \(Updated\)](#)
 - [cPanel Cross-Site Scripting](#)
 - [LibAST Buffer Overflow \(Updated\)](#)
 - [FreeBSD TCP SACK Remote Denial of Service](#)
 - [HP Tru64 DNS BIND Remote Unauthorized Access](#)
 - [IPsec-Tools ISAKMP IKE Remote Denial of Service \(Updated\)](#)
 - [Mailback Mail Header Injection](#)
 - [MPlayer Integer Overflows](#)
 - [Multiple Vendors Linux Kernel Coda Pioctl Local Buffer Overflow \(Updated\)](#)
 - [Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities \(Updated\)](#)
 - [Multiple Vendors Linux Kernel 'SEARCH_BINARY_HANDLER' Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel IPV6 Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel EXT2 File System Information Leak \(Updated\)](#)
 - [Multiple Vendors Linux Kernel ICMP Error Handling Remote Denial of Service](#)
 - [Multiple Vendors Linux Kernel Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel Remote Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel Denial of Service & Information Disclosure \(Updated\)](#)
 - [Multiple Vendors Linux Kernel 'Sysctl' Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel IPV6 FlowLabel Denial of Service \(Updated\)](#)
 - [Linux Kernel ZLib Invalid Memory Access Denial of Service \(Updated\)](#)
 - [Multiple Vendors Linux Kernel DM-Crypt Local Information Disclosure \(Updated\)](#)
 - [MyDNS Remote Denial of Service \(Updated\)](#)
 - [MyQuiz Arbitrary Shell Command Execution](#)
 - [NeoMail Cross-Site Scripting](#)
 - [Openwall 'crypt_blowfish' Information Disclosure](#)
 - [Powersave Elevated Privileges](#)
 - [Heimdal RSHD Server Elevated Privileges](#)
 - [Sun Java System Access Manager Authentication Bypass](#)
- Multiple Operating Systems
 - [Adobe Creative Suite File/Folder Elevated Privileges](#)
 - [ADODB PostgreSQL SQL Injection \(Updated\)](#)
 - [Apache mod_imap Cross-Site Scripting \(Updated\)](#)
 - [Blackboard Learning System Unauthorized Access \(Updated\)](#)
 - [Borland Delphi-BCB/Compiler Integer Overflow](#)
 - [CipherTrust IronMail Remote Denial of Service](#)
 - [Clever Copy SQL Injection](#)
 - [CyberShop Ultimate E-commerce Multiple Cross-Site Scripting](#)
 - [eyeOS PHP Code Execution](#)
 - [FFmpeg Remote Buffer Overflow \(Updated\)](#)
 - [Gallery Album Data Manipulation](#)
 - [Hinton Designs phphg Guestbook Multiple Vulnerabilities](#)
 - [IBM Tivoli Access Manager Directory Traversal](#)
 - [IBM Lotus Domino LDAP Server Denial of Service](#)
 - [Loudblog File Include](#)
 - [Mozilla History File Remote Denial of Service \(Updated\)](#)
 - [Multiple Mozilla Products Vulnerabilities](#)

- o [Multiple Vendors ADOdb Insecure Test Scripts \(Updated\)](#)
- o [MyBB 'posts' SQL Injection](#)
- o [Multiple PHP Vulnerabilities \(Updated\)](#)
- o [NukedWeb GuestBookHost SQL Injection](#)
- o [OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials \(Updated\)](#)
- o [Outblaze Cross-Site Scripting](#)
- o [PHP GEN SQL Injection & Cross-Site Scripting](#)
- o [PHP Multiple Vulnerabilities \(Updated\)](#)
- o [phpBB Information Disclosure](#)
- o [Phpclanwebsite SQL Injection \(Updated\)](#)
- o [PHP-Fusion Cross-Site Scripting](#)
- o [Pioneers Remote Denial of Service \(Updated\)](#)
- o [PluggedOut Blog SQL Injection & Cross-Site Scripting](#)
- o [QNX Neutrino RTOS Multiple Vulnerabilities](#)
- o [SoftMaker Shop Multiple Cross-Site Scripting](#)
- o [Sony Ericsson Cell Phones Bluetooth L2CAP Denial of Service](#)
- o [SPIP SQL Injection & Cross-Site Scripting \(Updated\)](#)
- o [Sun Java Web Start Sandbox Security Bypass](#)
- o [Sun Java JRE 'reflection' APIs Sandbox Security Bypass](#)
- o [Tachyondecay Vanilla Guestbook Multiple Input Validation](#)
- o [Unknown Domain Shoutbox Cross-Site Scripting & SQL Injection](#)
- o [vwdev SQL Injection](#)

[Wireless Trends & Vulnerabilities](#)

[General Trends](#)

[Viruses/Trojans](#)

Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. **Items in bold designate updates that have been made to past entries.** Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

The Risk levels are defined below:

High - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Medium - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

Low - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConflImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.

Windows Operating Systems Only				
Vendor & Software Name	Description	Common Name	CVSS	Resources
@Mail Webmail 4.3 for Windows	<p>A directory traversal vulnerability has been reported in @Mail Webmail that could let remote malicious users to execute arbitrary code.</p> <p>@Mail Workaround</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	@Mail Webmail Arbitrary Code Execution	Not Available	Secunia, Advisory: SA18646, February 2, 2006

Aquifer CMS	<p>A vulnerability has been reported in Aquifer CMS that could let remote malicious users conduct Cross-Site Scripting.</p> <p>Vendor solution available, contact vendor for details.</p> <p>There is no exploit code required.</p>	Aquifer CMS Cross Site Scripting CVE-2006-0122	2.3	<p>Security Focus, ID: 16162, January 6, 2006</p> <p>Security Focus, ID: 16162, February 7, 2006</p>
CommunityServer.org Community Server	<p>Multiple vulnerabilities have been reported in Community Server that could let remote malicious users conduct Cross-Site Scripting.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	Community Server Cross-Site Scripting CVE-2006-0535	2.3	Security Focus, ID: 16478, February 2, 2006
Computer Associates Unicenter TNG 2.1, 2.2, 2.4, 2.4.2	<p>A vulnerability has been reported in Unicenter TNG that could let remote malicious users cause a Denial of Service.</p> <p>Computer Associates</p> <p>There is no exploit code required.</p>	CA Unicenter TNG Denial of Service CVE-2006-0529 CVE-2006-0530	<p>2.3 (CVE-2006-0529)</p> <p>2.3 (CVE-2006-0530)</p>	Computer Associates, Security Notice, February 2, 2006
Hosting Controller 6.1 Hotfix 2.8	<p>An input validation vulnerability has been reported in Hosting Controller that could let malicious users perform SQL injection.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Hosting Controller SQL Injection CVE-2006-0581	4.2	Security Tracker, Alert ID: 1015584, February 6, 2006
Kinesphere eXchange POP3 prior to 5.0 b050203	<p>A buffer overflow vulnerability has been reported in eXchange POP3 that could let remote malicious users execute arbitrary code.</p> <p>eXchange POP3 Server 5.0 b060125</p> <p>A Proof of Concept exploit has been published.</p>	eXchange POP3 Arbitrary Code Execution CVE-2006-0537	7	Security Tracker, Alert ID: 1015580, February 3, 2006
Lexmark Printer Sharing Service	<p>A vulnerability has been reported in Lexmark Printer Sharing Service that could let remote malicious users execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	Lexmark Printer Sharing Service Arbitrary Code Execution CVE-2006-0592	7	Security Tracker, Alert ID: 1015593, February 7, 2006

Loftin Applications ASPSurvey	A vulnerability has been reported in ASPSurvey that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required.	Loftin Applications ASPSurvey Login.ASP SQL Injection Vulnerability CVE-2006-0192	7	Security Focus, ID: 16496, February 4, 2006
MailEnable Enterprise 1.2	A vulnerability has been reported in MailEnable that could let remote malicious users cause a Denial of Service. MailEnable Enterprise 1.2 Currently we are not aware of any exploits for this vulnerability.	MailEnable Enterprise Edition Webmail Denial of Service CVE-2006-0504	2.3	Secunia, Advisory: SA18716, February 7, 2006
Microsoft HTML Help Workshop 4.74.8702.0	A buffer overflow vulnerability has been reported in HTML Help Workshop that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft HTML Help Workshop Arbitrary Code Execution CVE-2006-0564	7	Secunia, Advisory: SA18740, February 6, 2006
Microsoft Internet Explorer 70. beta 2	A vulnerability has been reported in Internet Explorer, URLMon.DLL, that could let remote malicious users cause a Denial of Service or possibly execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Denial Of Service CVE-2006-0544	7	Security Focus, ID: 16463, February 1, 2006
Microsoft Internet Explorer various versions	A vulnerability has been reported in Internet Explorer that could let remote malicious users to execute arbitrary code. Microsoft Currently we are not aware of any exploits for this vulnerability.	Internet Explorer Arbitrary Code Execution CVE-2006-0020	7	Microsoft, Security Advisory 913333, February 7, 2006
Microsoft Windows XP SP1, Server 2003	A vulnerability has been reported in Windows, third party service configurations, that could let local malicious users obtain elevated privileges. Microsoft Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Privilege Elevation CVE-2006-0023	2.9	Microsoft, Security Advisory 914457, February 7, 2006 US-CERT VU#953860

Nullsoft Winamp 5.11 and prior	A vulnerability has been reported in Winamp that could let remote malicious users cause a Denial of Service. Winamp 5.13 Currently we are not aware of any exploits for this vulnerability.	Winamp Denial of Service CVE-2005-3188	7	Security Tracker, Alert ID: 1015565, February 2, 2006
Ritlabs The Bat! 2.12.04	A vulnerability has been reported in The Bat! that could let remote malicious users conduct spoofing. The Bat! version 3.5 or later Currently we are not aware of any exploits for this vulnerability.	The Bat! Spoofing	Not Available	Secunia, Advisory: SA18713, February 8, 2006
Symantec Sygate Management Server 4.1 b1417 and prior	An input validation vulnerability has been reported in Sygate Management Server that could let remote malicious users perform SQL injection or obtain unauthorized access. Symantec There is no exploit code required.	Symantec Sygate Management Server SQL Injection or Unauthorized Access CVE-2006-0522	7	Symantec, SYM06-002, February 1, 2006
Trend Micro ServerProtect 5.5.8	A vulnerability has been reported in ServerProtect that could let remote malicious users execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required.	Trend Micro ServerProtect Arbitrary Code Execution	Not Available	Security Focus, ID: 16483, February 3, 2006
WiredRed E/POP Web Conferencing 4.1.0.755	A vulnerability has been reported in E/POP Web Conferencing that could let remote malicious users perform HTML injection. No workaround or patch available at time of publishing. There is no exploit code required.	WiredRed E/POP Web Conferencing HTML Injection	Not Available	Security Focus, ID: 16542, February 8, 2006

[\[back to top\]](#)

UNIX / Linux Operating Systems Only

Vendor & Software Name	Description	Common Name	CVSS	Resources
BlueZ Project hcidump 1.29	A remote Denial of Service vulnerability has been reported in 'l2cap.c' due to an error when handling L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.	hcidump Bluetooth L2CAP Remote Denial of Service	Not Available	Secunia Advisory: SA18741, February 8, 2006

	<p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit script, hcidump-crash.c, has been published.</p>			
<p>Bogofilter Email Filter</p> <p>Bogofilter Email Filter 0.96.2, 0.95.2, 0.94.14, 0.94.12, 0.93.5</p>	<p>Several buffer overflow vulnerabilities have been reported: a vulnerability was reported in bogofilter and bogolexer when character set conversion is performed on invalid input sequences, which could let a remote malicious user cause a Denial of Service; and a vulnerability was reported in bogofilter and bogolexer when processing input that contains overly long words, which could let a remote malicious user cause a Denial of Service.</p> <p>Upgrade available</p> <p>Ubuntu</p> <p>SuSE</p> <p>There is no exploit code required.</p>	<p>Bogofilter Multiple Remote Buffer Overflows</p> <p>CVE-2005-4591 CVE-2005-4592</p>	<p>7 (CVE-2005-4591)</p> <p>7 (CVE-2005-4592)</p>	<p>Bogofilter Security Advisories, bogofilter-SA-2005-01 & 02, January 2, 2006</p> <p>Ubuntu Security Notice, USN-240-1, January 11, 2006</p> <p>SuSE Security Summary Report, SUSE-SR:2006:003, February 3, 2006</p>
<p>cPanel, Inc.</p> <p>cPanel 10</p>	<p>Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified user-supplied input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported in 'mime/handle.html' due to insufficient sanitization of the 'extension' and 'mime-type' parameters, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>cPanel Cross-Site Scripting</p> <p>CVE-2006-0573 CVE-2006-0574</p>	<p>2.3 (CVE-2006-0573)</p> <p>2.3 (CVE-2006-0574)</p>	<p>Secunia Advisory: SA18695, February 7, 2006</p>
<p>ETERM</p> <p>LibAST prior to 0.7</p>	<p>A buffer overflow vulnerability has been reported in 'conf.c' due to a boundary error in the 'conf_find_file()' function, which could let a malicious user execute arbitrary code.</p> <p>Update available</p> <p>Gentoo</p> <p>Mandriva</p> <p>An exploit script, eterm-exploit.c, has been published.</p>	<p>LibAST Buffer Overflow</p> <p>CVE-2006-0224</p>	<p>4.9</p>	<p>Secunia Advisory: SA18586, January 25, 2006</p> <p>Gentoo Linux Security Advisory, GLSA 200601-14, January 29, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:029, February 2, 2006</p>

FreeBSD FreeBSD 5.4 -RELENG, -RELEASE, -PRERELEASE, STABLE, 5.3 -STABLE, -RELENG, -RELEASE	A remote Denial of Service vulnerability has been reported due to an error in SACK (Selective ACKnowledgement) handling. Patches available There is no exploit code required.	FreeBSD TCP SACK Remote Denial of Service CVE-2006-0433	2.3	FreeBSD Security Advisory, FreeBSD-SA-06:08, February 1, 2006
Hewlett Packard Company Tru64 5.1 B-3, B-2 PK4, 5.1 A PK6, 4.0 G PK4, 4.0 F PK8	A vulnerability has been reported due to an unspecified error in DNS BIND, which could let a remote malicious user obtain unauthorized access. Patches available Currently we are not aware of any exploits for this vulnerability.	HP Tru64 DNS BIND Remote Unauthorized Access CVE-2006-0527	7	HP Security Bulletin, HPSBTU02095, January 31, 2006
IPsec-Tools IPsec-Tools0.6-0.6.2, 0.5-0.5.2	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions when in 'AGGRESSIVE' mode. IpsecTools Ubuntu Gentoo SUSE Conectiva Mandriva Debian Vulnerability can be reproduced with the PROTOS IPSec Test Suite.	IPsec-Tools ISAKMP IKE Remote Denial of Service CVE-2005-3732	5	Security Focus, Bugtraq ID: 15523, November 22, 2005 Ubuntu Security Notice, USN-221-1, December 01, 2005 Gentoo Linux Security Advisory, GLSA 200512-04, December 12, 2005 SUSE Security Announcement, SUSE-SA:2005:070, December 20, 2005 Conectiva Linux Announcement, CLSA-2006:1058, January 2, 2006 Mandriva Security Advisory, MDKSA-2006:020, January 25, 2006 Debian Security Advisory, DSA-965-1, February 6, 2006
Mailback mailback.pl 1.3.	A vulnerability has been reported due to insufficient sanitization of the 'subject' parameter before used to construct an email message, which could let a remote malicious user bypass security restrictions. Update available Currently we are not aware of any exploits for this vulnerability.	Mailback Mail Header Injection	Not Available	Secunia Advisory: SA18748, February 7, 2006

MPlayer MPlayer 1.0pre7try2	Integer overflow vulnerabilities have been reported in the 'new_demux_packet()' function in 'libmpdemux/demuxer.h' and the 'demux_asf_read_packet()' function in 'libmpdemux/demux_asf.c' when allocating memory, which could let a remote malicious user cause a Denial of Service and potentially compromise a system. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	MPlayer Integer Overflows CVE-2006-0579	7	Secunia Advisory: SA18718, February 7, 2006
Multiple Vendors Linux kernel 2.6-2.6.10, 2.4-2.4.28	A buffer overflow vulnerability has been reported in the 'coda_pioclt' function of the 'pioctl.c' file, which could let a malicious user cause a Denial of Service or execute arbitrary code with superuser privileges. RedHat RedHat Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Coda_Pioclt Local Buffer Overflow CVE-2005-0124	2.3	Security Focus, Bugtraq ID: 14967, September 28, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 RedHat Security Advisory, RHSA-2006:0191-9, February 1, 2006
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora Ubuntu Fedora RedHat Conectiva FedoraLegacy RedHat RedHat RedHat Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CVE-2005-0815	6.7	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005 Fedora Legacy Update Advisory, FLISA:152532, June 4, 1005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006

Multiple Vendors Linux Kernel 2.4- 2.4.32	<p>A Denial of Service vulnerability has been reported due to insufficient validation of the return code of a function call in the 'search_binary_handler()' function.</p> <p>Updates available</p> <p>RedHat</p> <p>RedHat</p> <p>A Proof of Concept exploit has been published.</p>	<p>Linux Kernel 'SEARCH_BINARY_HANDLER' Denial of Service</p> <p>CVE-2005-2708</p>	2.3	<p>Security Focus, Bugtraq ID: 16320, January 19, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0190-5, February 1, 2006</p>
Multiple Vendors Linux kernel 2.6- 2.6.14	<p>A Denial of Service vulnerability has been reported in 'net/ipv6/udp.c' due to an infinite loop error in the 'udp_v6_get_port()' function.</p> <p>Fedora</p> <p>Upgrades available</p> <p>Ubuntu</p> <p>SUSE</p> <p>RedHat</p> <p>RedHat</p> <p>RedHat</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel IPV6 Denial of Service</p> <p>CVE-2005-2973</p>	2.3	<p>Secunia Advisory: SA17261, October 21, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1007 & 1013, October 20, 2005</p> <p>Security Focus, Bugtraq ID: 15156, October 31, 2005</p> <p>Ubuntu Security Notice, USN-219-1, November 22, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006</p>
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1-2.6.11; RedHat Fedora Core2	<p>A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information.</p> <p>Patches available</p> <p>Fedora</p> <p>Trustix</p> <p>Fedora</p> <p>RedHat</p> <p>Conectiva</p> <p>FedoraLegacy</p> <p>SUSE</p> <p>RedHat</p> <p>RedHat</p>	<p>Linux Kernel EXT2 File System Information Leak</p> <p>CVE-2005-0400</p>	2.3	<p>Security Focus, 12932, March 29, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005</p> <p>Fedora Update Notification FEDORA-2005-313, April 11, 2005</p> <p>RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005</p> <p>Conectiva Linux Security Announcement, CLA-2005:952, May 2,</p>

	RedHat Currently we are not aware of any exploits for this vulnerability.			2005 Fedora Legacy Update Advisory, FLSA:152532, June 4, 1005 SUSE Security Announcement, SUSE-SA:2005:029, June 9, 2005 RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006
Multiple Vendors Linux Kernel 2.6.x; RedHat Fedora Core4	A remote Denial of Service vulnerability has been reported in the 'ip_options_echo()' function due to an error when constructing an ICMP response. Updates available Fedora Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ICMP Error Handling Remote Denial of Service CVE-2006-0454	2.3	Secunia Advisory: SA18766, February 8, 2006
Multiple Vendors Linux kernel 2.6-2.6.12.3, 2.4-2.4.32	A Denial of Service vulnerability has been reported in 'IP_VS_CONN_FLUSH' due to a NULL pointer dereference. Kernel versions 2.6.13 and 2.4.32-pre2 are not affected by this issue. Ubuntu Mandriva Debian Conectiva RedHat Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Denial of Service CVE-2005-3274	2.3	Security Focus, Bugtraq ID: 15528, November 22, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005 Debian Security Advisory, DSA 922-1, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisory, RHSA-2006:0190-5, February 1, 2006

<p>Multiple Vendors</p> <p>Linux kernel 2.6-2.6.12, 2.4-2.4.31</p>	<p>A remote Denial of Service vulnerability has been reported due to a design error in the kernel.</p> <p>The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue.</p> <p>Ubuntu</p> <p>Mandriva</p> <p>SUSE</p> <p>Conectiva</p> <p>RedHat</p> <p>RedHat</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel Remote Denial of Service</p> <p>CVE-2005-3275</p>	<p>3.3</p>	<p>Ubuntu Security Notice, USN-219-1, November 22, 2005</p> <p>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005</p> <p>Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006</p>
--	--	---	----------------------------	---

<p>Multiple Vendors</p> <p>Linux kernel 2.6-2.6.14</p>	<p>Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in 'security/keys/request_key_auth.c'; a Denial of Service vulnerability was reported due to a memory leak in 'fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information.</p> <p>Linux Kernel</p> <p>Fedora</p> <p>Trustix</p> <p>RedHat</p> <p>Ubuntu</p> <p>Mandriva</p> <p>SUSE</p> <p>Conectiva</p> <p>RedHat</p> <p>RedHat</p> <p>RedHat</p> <p>There is no exploit code required.</p>	<p>Linux Kernel Denial of Service & Information Disclosure</p> <p>CVE-2005-3119</p> <p>CVE-2005-3180</p> <p>CVE-2005-3181</p>	<p>2.3 (CVE-2005-3119)</p> <p>3.3 (CVE-2005-3180)</p> <p>2.3 (CVE-2005-3181)</p>	<p>Secunia Advisory: SA17114, October 12, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0057, October 14, 2005</p> <p>Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005</p> <p>RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005</p> <p>Ubuntu Security Notice, USN-219-1, November 22, 2005</p> <p>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005</p> <p>Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006</p> <p>RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006</p>
--	---	---	--	---

Multiple Vendors Linux kernel 2.6-2.6.14	A Denial of Service vulnerability has been in 'sysctl.c' due to an error when handling the un-registration of interfaces in '/proc/sys/net/ipv4/conf/'. Upgrades available Ubuntu RedHat RedHat RedHat RedHat There is no exploit code required.	Linux Kernel 'Sysctl' Denial of Service CVE-2005-2709	4.9	Secunia Advisory: SA17504, November 9, 2005 Ubuntu Security Notice, USN-219-1, November 22, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006
Multiple Vendors SuSE Linux Professional 10.0 OSS, 10.0, Personal 10.0 OSS; Linux kernel 2.6-2.6.13, Linux kernel 2.4-2.4.32	A Denial of Service vulnerability has been reported in FlowLable. Upgrades available SUSE RedHat Mandriva RedHat RedHat Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPv6 FlowLable Denial of Service CVE-2005-3806	5.3	Security Focus, Bugtraq ID: 15729, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 RedHat Security Advisory, RHSA-2006:0101-9, January 17, 2006 RedHat Security Advisory, RHSA-2006:0140-9, January 19, 2006 Mandriva Security Advisory, MDKSA-2006:018, January 20, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0; SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9;	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions. Linux Kernel Ubuntu SUSE Trustix Mandriva Mandriva: SUSE: Conectiva	Linux Kernel ZLib Invalid Memory Access Denial of Service CVE-2005-2458	3.3	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TLSA-2005-0043, September 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005 Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30,

Linux kernel 2.6-2.6.12.4	RedHat RedHat Currently we are not aware of any exploits for this vulnerability.			2005 SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005 Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006 RedHat Security Advisories, RHSA-2006:0190-5 & RHSA-2006:0191-9, February 1, 2006
Multiple Vendors Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.15	A vulnerability has been reported in the 'cm-crypt' driver due to a failure to clear memory, which could let a malicious user obtain sensitive information. Updates available Ubuntu Trustix Fedora Currently we are not aware of any exploits for this vulnerability.	Linux Kernel DM-Crypt Local Information Disclosure CVE-2006-0095	1.6	Security Focus, Bugtraq ID: 16301, January 18, 2006 Ubuntu Security Notice, USN-244-1 January 18, 2006 Trustix Secure Linux Security Advisory, TSLSA-2006-0004, January 27, 2006 Secunia Advisory: SA18774, February 8, 2006
MyDNS MyDNS 1.0.0	A remote Denial of Service vulnerability has been reported due to an error when handling certain malformed DNS queries. Update available Gentoo Debian Currently we are not aware of any exploits for this vulnerability.	MyDNS Remote Denial of Service CVE-2006-0351	2.3	Security Tracker Alert ID: 1015521, January 20, 2006 Gentoo Linux Security Advisory, GLSA 200601-16, January 30, 2006 Debian Security Advisory, DSA-963-1, February 2, 2006
MyQuiz MyQuiz 1.01	A vulnerability has been reported in 'myquiz.pl' due to insufficient sanitization of the 'ENV{'PATH_INFO'}' variable, which could let a remote malicious user execute arbitrary shell commands. No workaround or patch available at time of publishing. A Proof of Concept exploit script, myquiz101.pl.txt, has been published.	MyQuiz Arbitrary Shell Command Execution	Not Available	Secunia Advisory: SA18737, February 6, 2006
NeoCode Solutions NeoMail	A Cross-Site Scripting vulnerability has been in the 'neomail.pl' script due to insufficient sanitization of the 'date' parameter before displaying the input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	NeoMail Cross-Site Scripting CVE-2006-0536	2.3	Security Tracker Alert ID: 1015581, February 3, 2006

Openwall Openwall crypt_blowfish 0.4.7 & prior	A vulnerability has been reported in 'crypt_gensalt.c' due to signedness errors, which could let a remote malicious user obtain sensitive information. Updates available Currently we are not aware of any exploits for this vulnerability.	Openwall 'crypt_blowfish' Information Disclosure	Not Available	Secunia Advisory: SA18772, February 8, 2006
Powersave Powersave 0.11, 0.10.15	A vulnerability has been reported when handling a powersave action sent by a client, which could let a malicious user obtain elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	Powersave Elevated Privileges CVE-2006-0612	Not Available	Secunia Advisory: SA18651, February 2, 2006
Royal Institute of Technology Heimdal prior to 0.6.6 & 0.7.2	A vulnerability has been reported in the 'rshd' server when storing forwarded credentials due to an unspecified error, which could let a malicious user obtain elevated privileges. Update to version 0.7.2 or 0.6.6. Currently we are not aware of any exploits for this vulnerability.	Heimdal RSHD Server Elevated Privileges CVE-2006-0582	1.6	Security Tracker Alert ID: 1015591, February 7, 2006
Sun Microsystems, Inc. Java System Access Manager 7.0 2005Q4 Solaris x, Solaris S, Linux	A vulnerability has been reported due to a failure to require proper credentials, which could let a malicious user bypass authentication. Patches available There is no exploit code required.	Sun Java System Access Manager Authentication Bypass CVE-2006-0531	7	Sun Alert ID 102140, February 1, 2006

[\[back to top\]](#)

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Description	Common Name	CVSS	Resources
Adobe Creative Suite 2, Adobe Photoshop CS2, Adobe Illustrator CS2 Creative Suite	A vulnerability has been reported due to insecure default file permissions on installed files and folders, which could let a malicious user obtain elevated privileges Patch information Currently we are not aware of any exploits for this vulnerability.	Adobe Creative Suite File/Folder Elevated Privileges CVE-2006-0525	4.9	Adobe Security Advisory, February 2, 2006
ADOdb ADOdb 4.70, 4.68, 4.66	An SQL injection vulnerability has been reported due to insufficient sanitization of certain parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Updates available Gentoo	ADOdb PostgreSQL SQL Injection CVE-2006-0410	2.3	Secunia Advisory: SA18575, January 24, 2006 Gentoo Linux Security Advisory, GLSA 200602-02, February 6, 2006

	There is no exploit code required.			
<p>Apache Software Foundation</p> <p>Apache prior to 1.3.35-dev, 2.0.56-dev</p>	<p>A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev.</p> <p>OpenPKG</p> <p>Trustix</p> <p>Mandriva</p> <p>Ubuntu</p> <p>RedHat</p> <p>Fedora</p> <p>TurboLinux</p> <p>Gentoo</p> <p>There is no exploit code required.</p>	<p>Apache mod_imap Cross-Site Scripting</p> <p>CVE-2005-3352</p>	<p>2.3</p>	<p>Security Tracker Alert ID: 1015344, December 13, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005</p> <p>Trustix Secure Linux Security Advisory, TLSA-2005-0074, December 23, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2006:007, January 6, 2006</p> <p>Ubuntu Security Notice, USN-241-1, January 12, 2006</p> <p>RedHat Security Advisory, RHSA-2006:0158-4, January 17, 2006</p> <p>Fedora Security Advisory, FEDORA-2006-052, January 23, 2006</p> <p>Turbolinux Security Advisory, TLSA-2006-1, January 25, 2006</p> <p>Gentoo Linux Security Advisory, GLSA 200602-03, February 6, 2006</p>
<p>Blackboard</p> <p>Blackboard Academic Suite 6.0, Blackboard 6.0, 5.5.1, 5.5, 5.0.2, 5.0</p>	<p>A vulnerability has been reported in the authentication mechanism, which could let a malicious user obtain unauthorized access. NOTE: the vendor has disputed this issue, saying that "This is a customer specific issue related to their Kerberos authentication single sign-on application and not a vulnerability in the Blackboard product."</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>Blackboard Learning System Unauthorized Access</p> <p>CVE-2006-0511</p>	<p>2.9</p>	<p>Security Focus, Bugtraq ID: 16438, January 31, 2006</p> <p>Security Focus, Bugtraq ID: 16438, February 7, 2006</p>
<p>Borland</p> <p>BCB6 ent_upd4</p>	<p>A integer overflow vulnerability has been reported because statements that use the 'sizeof' operator are not correctly compiled, which could let a malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Borland Delphi-BCB/Compiler Integer Overflow</p>	<p>Not available</p>	<p>XFocus Security Team Advisory, xfocus-SD-060206, February 6, 2006</p>
<p>Cipher Trust</p> <p>IronMail 5.0.1</p>	<p>A remote Denial of Service vulnerability has been reported if configured with 'Denial of Service Protection' enabled when dealing</p>	<p>CipherTrust IronMail Remote Denial of Service</p>	<p>2.3</p>	<p>Security Tracker Alert ID: 1015555, February 1, 2006</p>

	<p>with SYN flood attacks.</p> <p>The vendor has released an update to address this issue. Contact the vendor for further information.</p> <p>There is no exploit code required.</p>	CVE-2006-0538		
<p>Clever Copy</p> <p>Clever Copy 3.0</p>	<p>An SQL injection vulnerability has been reported in the 'mailarticle.php' script due to insufficient validation of the 'ID' parameter, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Exploit details, Clever_Copy_V3_sql.txt, have been published.</p>	<p>Clever Copy SQL Injection</p> <p>CVE-2006-0583</p>	7	Security Tracker Alert ID: 1015590, February 7, 2006
<p>CyberShop ASP</p> <p>Ultimate E-commerce Script 0</p>	<p>Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>	<p>CyberShop Ultimate E-commerce Multiple Cross-Site Scripting</p> <p>CVE-2006-0534</p>	2.3	Security Focus, Bugtraq ID: 16473, February 2, 2006
<p>eyeOS</p> <p>eyeOS 0.8.9 & prior</p>	<p>A vulnerability has been reported caused due to incorrectly initialized sessions, which could let a remote malicious user execute arbitrary PHP code.</p> <p>Updates available</p> <p>Currently we are not aware of any exploits for this vulnerability</p>	eyeOS PHP Code Execution	Not available	GulfTech Security Research Team Advisory, February 8, 2006
<p>FFmpeg</p> <p>FFmpeg 0.4.9-pre1, 0.4.6-0.4.8, FFmpeg CVS</p>	<p>A buffer overflow vulnerability has been reported in the 'avcodec_default_get_buffer()' function of 'utils.c' in libavcodec due to a boundary error, which could let a remote malicious user execute arbitrary code.</p> <p>Patches available</p> <p>Ubuntu</p> <p>Mandriva</p> <p>Ubuntu</p> <p>Gentoo</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>FFmpeg Remote Buffer Overflow</p> <p>CVE-2005-4048</p>	7	<p>Secunia Advisory: SA17892, December 6, 2005</p> <p>Ubuntu Security Notice, USN-230-1, December 14, 2005</p> <p>Mandriva Linux Security Advisories MDKSA-2005:228-232, December 15, 2005</p> <p>Ubuntu Security Notice, USN-230-2, December 16, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200602-01, February 5, 2006</p>
<p>Gallery Project</p> <p>Gallery 1.5.2.</p>	<p>A vulnerability has been reported due to an unspecified error, which could let a remote malicious user manipulate stored album data.</p> <p>Update available</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Gallery Album Data Manipulation</p> <p>CVE-2006-0587</p>	4.2	Secunia Advisory: SA18735, February 7, 2006

Hinton Design phphg Guestbook 1.2	Multiple vulnerabilities have been reported: SQL injection vulnerabilities were reported in 'check.php' due to insufficient sanitization of the 'username' parameter during login and in the 'id' parameter in the administration section, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of various fields when signing the guestbook, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to an insecure authentication process, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	phphg Guestbook Multiple Vulnerabilities CVE-2006-0602 CVE-2006-0603 CVE-2006-0604	Not Available	Security Focus, Bugtraq ID: 16541, February 8, 2006
IBM Tivoli Access Manager for e-business 5.1.0, 6.0	A Directory Traversal vulnerability has been reported in 'pkmslogout' due to insufficient sanitization of the 'filename' parameter before using to retrieve the page template, which could let a remote malicious user obtain sensitive information. Patches available (5.1.0) Patches available (6.0) There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM Tivoli Access Manager Directory Traversal CVE-2006-0513	2.3	Virtual Security Research, LLC. Advisory, February 3, 2006
IBM Lotus Domino 7.0	A Denial of Service vulnerability has been reported in the LDAP server when handling certain requests. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	IBM Lotus Domino LDAP Server Denial of Service CVE-2006-0580	2.3	Secunia Advisory: SA18738, February 7, 2006
Loudblog Loudblog 0.4	A file include vulnerability has been reported in 'loudblog/inc/backend_settings.php' due to insufficient verification of the 'path' parameter before using to include files, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. A Proof of Concept exploit script, loudblog_04_incl_xpl.php, has been published.	Loudblog File Include CVE-2006-0565	7	Security Tracker Alert ID: 1015583, February 4, 2006
Mozilla Firefox 1.5, Netscape Browser 8.0.4; Netscape Browser 8.0.4	A remote Denial of Service vulnerability has been reported when handling large history information. <i>Note: The vendor disputes this claim.</i> Netscape Mozilla RedHat	Mozilla History File Remote Denial of Service CVE-2005-4134	2.3	Secunia Advisory: SA17934, December 8, 2005 Security Focus, Bugtraq ID: 15773, January 27, 2006 Mozilla Foundation Security Advisory 2006-03, February 1,

	RedHat Fedora Mandriva Mandriva A Proof of Concept exploit script has been published.			2006 RedHat Security Advisories, RHSA-2006-0199 & RHSA-2006:0200-8, February 2, 2006 RedHat Fedora Security Advisories, FEDORA-2006-075 & FEDORA-2006-076, February 3, 2006 Mandriva Security Advisories, MDKSA-2006:036 & MDKSA-2006:037, February 7, 2006
Multiple Vendors Mozilla Browser 0.8-0.9.9, 0.9.35, 0.9.48, 1.0-1.7.12, Thunderbird 0.x, 1.x, Firefox 0.x, 1.x; SeaMonkey 1.0; RedHat Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, ES 2.1, AS 4, AS 3, AS 2.1 IA64, AS 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1	Multiple vulnerabilities have been reported: vulnerabilities were reported because temporary variables that are not properly protected are used in the JavaScript engine's garbage collection, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported because a remote malicious user can create HTML that will dynamically change the style of an element from position:relative to position:static; a vulnerability was reported because a remote malicious user can create HTML that invokes the QueryInterface() method of the built-in Location and Navigator objects; a vulnerability was reported in the 'XULDocument.persist()' function due to improper validation of the user-supplied attribute name, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability was reported in the 'E4X,' 'SVG,' and 'Canvas' features, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the XML parser because data can be read from locations beyond the end of the buffer, which could lead to a Denial of Service; and a vulnerability was reported because the 'E4X' implementation's internal 'AnyName' object is incorrectly available to web content, which could let a remote malicious user bypass same-origin restrictions. Mozilla RedHat RedHat Fedora Mandriva Mandriva There is no exploit code required for some of these vulnerabilities; however, an exploit, firefox_queryinterface.pm, has been	Multiple Mozilla Products Vulnerabilities CVE-2006-0292 CVE-2006-0293 CVE-2006-0294 CVE-2006-0295 CVE-2006-0296 CVE-2006-0297 CVE-2006-0298 CVE-2006-0299	7 (CVE-2006-0292) 7 (CVE-2006-0293) 7 (CVE-2006-0294) 3.9 (CVE-2006-0295) 2.3 (CVE-2006-0296) 7 (CVE-2006-0297) 2.3 (CVE-2006-0298) 4.7 (CVE-2006-0299)	Mozilla Foundation Security Advisories 2006-01-2006-08, February 1, 2006 RedHat Security Advisories, RHSA-2006:0199-10 & RHSA-2006:0200-8, February 2, 2006 Fedora Security Advisories, FEDORA-2006-075 & FEDORA-2006-076, February 2, 2006 US-CERT VU#592425 US-CERT VU#759273 Mandriva Security Advisories, MDKSA-2006:036 & MDKSA-2006:037, February 7, 2006

	published.			
Multiple Vendors PostNuke Development Team PostNuke 0.761; moodle 1.5.3; Mantis 1.0.0RC4, 0.19.4; Cacti 0.8.6 g; ADOdb 4.68, 4.66; AgileBill 1.4.92 & prior	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'server.php' test script, which could let a remote malicious user execute arbitrary SQL code and PHP script code; and a vulnerability was reported in the 'tests/tmssql.php' text script, which could let a remote malicious user call an arbitrary PHP function.</p> <p>Adodb</p> <p>Cacti</p> <p>Moodle</p> <p>PostNuke</p> <p>AgileBill</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	ADODB Insecure Test Scripts CVE-2006-0146 CVE-2006-0147	7 (CVE-2006-0146) 7 (CVE-2006-1047)	<p>Secunia Advisory: SA17418, January 9, 2006</p> <p>Security Focus, Bugtraq ID: 16187, February 7, 2006</p>
MyBB Group MyBB (formerly MyBulletinBoard) 1.03	<p>An SQL injection vulnerability has been reported in 'moderation.php' due to insufficient sanitization of the 'posts' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	MyBB 'posts' SQL Injection	Not Available	Secunia Advisory: SA18754, February 8, 2006
NukedWeb GuestBookHost	<p>SQL injection vulnerabilities have been reported in 'config.php' due to insufficient sanitization of the 'email' and 'password' fields before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	GuestBookHost SQL Injection CVE-2006-0542	7	Secunia Advisory: SA18761, February 8, 2006
OpenSSH OpenSSH 4.1, 4.0, p1	<p>Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials.</p> <p>OpenBSD</p> <p>Fedora</p> <p>Trustix</p> <p>Slackware</p> <p>Fedora</p>	<p>OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials</p> <p>CVE-2005-2797 CVE-2005-2798</p>	<p>3.3 (CVE-2005-2797)</p> <p>3.3 (CVE-2005-2798)</p>	<p>Secunia Advisory: SA16686, September 2, 2005</p> <p>Fedora Update Notification, FEDORA-2005-858, September 7, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005</p> <p>Slackware Security Advisory, SSA:2005-251-03, September 9, 2005</p> <p>Fedora Update Notification, FEDORA-2005-860, September 12, 2005</p>

	RedHat Mandriva Ubuntu Conectiva HP Avaya SuSE <p>There is no exploit code required.</p>			<p>RedHat Security Advisory, RHSA-2005:527-16, October 5, 2005</p> <p>Mandriva Linux Security Update Advisory, MDKSA-2005:172, October 6, 2005</p> <p>Ubuntu Security Notice, USN-209-1, October 17, 2005</p> <p>Conectiva Linux Announcement, CLSA-2005:1039, October 19, 2005</p> <p>Security Focus, Bugtraq ID: 14729, January 10, 2006</p> <p>Avaya Security Advisory, ASA-2006-033, January 30, 2006</p> <p>SuSE Security Summary Report, SUSE-SR:2006:003, February 3, 2006</p>
Outblaze Ltd. Outblaze	<p>A Cross-Site Scripting vulnerability has been reported in 'throw.main' due to insufficient sanitization of the 'file' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>A Proof of Concept exploit has been published.</p>	Outblaze Cross-Site Scripting CVE-2006-0568	2.3	Secunia Advisory: SA18710, February 3, 2006
PHP GEN PHP GEN 1.3	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of unspecified input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Update available</p> <p>There is no exploit code required.</p>	PHP GEN SQL Injection & Cross-Site Scripting CVE-2006-0497	7	Secunia Advisory: SA18715, February 3, 2006
PHP PHP 4.0.x, 4.1.x, 4.2.x, 4.3.x, 4.4.x, 5.0.x	<p>Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of the 'GLOBALS' array, which could let a remote malicious user define global variables; a vulnerability was reported in the 'parse_str()' PHP function when handling an unexpected termination, which could let a remote malicious user enable the 'register_globals' directive; a Cross-Site Scripting vulnerability was reported</p>	<p>PHP Multiple Vulnerabilities</p> <p>CVE-2005-3388 CVE-2005-3389 CVE-2005-3390 CVE-2005-3391 CVE-2005-3392</p>	<p>3.3 (CVE-2005-3388)</p> <p>3.3 (CVE-2005-3389)</p> <p>8 (CVE-2005-3390)</p> <p>7 (CVE-2005-3391)</p> <p>7</p>	<p>Secunia Advisory: SA17371, October 31, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005</p> <p>Turbolinux Security Advisory TLSA-2005-97, November 5, 2005</p>

	<p>in the 'phpinfo()' PHP function due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an integer overflow vulnerability was reported in 'pcrelib' due to an error, which could let a remote malicious user corrupt memory.</p> <p>Upgrades available</p> <p>SUSE</p> <p>TurboLinux</p> <p>Fedora</p> <p>RedHat</p> <p>RedHat</p> <p>Gentoo</p> <p>Mandriva</p> <p>SUSE</p> <p>Trustix</p> <p>SGI</p> <p>OpenPKG</p> <p>Ubuntu</p> <p>Avaya</p> <p>Mandriva</p> <p>There is no exploit code required.</p>		(CVE-2005-3392)	<p>Fedora Update Notifications, FEDORA-2005-1061 & 1062, November 8, 2005</p> <p>RedHat Security Advisories, RHSA-2005:838-3 & RHSA-2005:831-15, November 10, 2005</p> <p>Gentoo Linux Security Advisory, GLSA 200511-08, November 13, 2005</p> <p>Mandriva Linux Security Advisory, MDKSA-2005:213, November 16, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:027, November 18, 2005</p> <p>Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005</p> <p>SGI Security Advisory, 20051101-01-U, November 29, 2005</p> <p>OpenPKG Security Advisory, OpenPKG-SA-2005.027, December 3, 2005</p> <p>SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005</p> <p>SUSE Security Announcement, SUSE-SA:2005:069, December 14, 2005</p> <p>Ubuntu Security Notice, USN-232-1, December 23, 2005</p> <p>Avaya Security Advisory, ASA-2006-037, January 31, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:035, February 7, 2006</p>
<p>PHP</p> <p>PHP 5.1.1, 5.1</p>	<p>Several vulnerabilities have been reported: a vulnerability was reported due to insufficient of the session ID in the session extension before returning to the user, which could let a remote malicious user inject arbitrary HTTP headers; a format string vulnerability was reported in the 'mysqli' extension when processing error messages, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insufficient sanitization of unspecified input that is passed</p>	<p>Multiple PHP</p> <p>CVE-2006-0207</p> <p>CVE-2006-0208</p>	<p>2.3</p> <p>(CVE-2006-0208)</p>	<p>Secunia Advisory: SA18431, January 13, 2006</p> <p>Mandriva Security Advisory, MDKSA-2006:028, February 1, 2006</p>

	<p>under certain error conditions, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>PHP</p> <p>Mandriva</p> <p>There is no exploit code required.</p>			
<p>phpBB Group</p> <p>phpBB 2.0.1-2.0.19</p>	<p>A vulnerability has been reported in the 'Referer' HTTP header when certain requests are sent for external avatar images and certain BBcode that references external web sites, which could let a remote malicious user obtain sensitive information.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>phpBB Information Disclosure</p> <p>CVE-2006-0437 CVE-2006-0438</p>	<p>2.3 (CVE-2006-0437)</p> <p>2.3 (CVE-2006-0438)</p>	<p>Secunia Advisory: SA18693, February 6, 2006</p>
<p>Phpclanwebsite</p> <p>Phpclanwebsite 1.23.1</p>	<p>SQL injection vulnerabilities have been reported in 'index.php' due to insufficient sanitization of the 'par' and 'poll_id' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>Update available</p> <p>There is no exploit code required; however, a Proof of Concept exploit script, Phpclanwebsite.1.23.1.SQL.Injection.pl, has been published.</p>	<p>Phpclanwebsite SQL Injection</p> <p>CVE-2006-0444</p>	<p>7</p>	<p>Security Focus, Bugtraq ID: 16391, January 26, 2006</p> <p>Security Focus, Bugtraq ID: 16391, January 30, 2006</p>
<p>PHP-Fusion</p> <p>PHP-Fusion 6.0.204, 6.0.110, 6.0.109, 6.0.107, 6.0.105, 6.0.0.3, 6.0.206, 6.0.106, 5.0.1 Service Pack, 5.0, 4.0.1, 4.00</p>	<p>Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'shout_name' field in 'shoutbox_panel.php' and in the 'comments' field in 'comments_include.php,' which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>Updates available</p> <p>There is no exploit code required.</p>	<p>PHP-Fusion Cross-Site Scripting</p> <p>CVE-2006-0593</p>	<p>2.3</p>	<p>Security Focus, Bugtraq ID: 16548, February 8, 2006</p>
<p>Pioneers</p> <p>Pioneers 0.9.40</p>	<p>A remote Denial of Service vulnerability has been reported due to a boundary error when handling overly long chat messages.</p> <p>Update available</p> <p>Debian</p> <p>There is no exploit code required.</p>	<p>Pioneers Remote Denial of Service</p> <p>CVE-2006-0467</p>	<p>2.3</p>	<p>Security Focus, Bugtraq ID: 16429, January 30, 2006</p> <p>Debian Security Advisory, DSA-964-1, February 3, 2006</p>
<p>PluggedOut</p> <p>PluggedOut Blog 1.x</p>	<p>Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'exec.php' due to insufficient sanitization of the 'entryid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'problem.php' due to insufficient sanitization of the 'data' parameter before returning to the user, which</p>	<p>PluggedOut Blog SQL Injection & Cross-Site Scripting</p> <p>CVE-2006-0562 CVE-2006-0563</p>	<p>2.3 (CVE-2006-0562)</p> <p>7 (CVE-2006-0563)</p>	<p>Security Tracker Alert ID: 1015586, February 6, 2006</p>

	<p>could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, Proof of Concept exploits have been published.</p>			
<p>QNX Software Systems</p> <p>QNX Neutrino RTOS 6.x</p>	<p>Multiple vulnerabilities have been reported: a vulnerability was reported in the 'crtrap' utility because libraries are loaded insecurely, which could let a malicious user obtain elevated privileges; a format string vulnerability was reported in the 'fontsluth' utility, which could let a malicious user execute arbitrary code; a vulnerability was reported in the '_ApFindTranslationFile()' function when handling the 'ABLPATH' environment variable due to a boundary error, which could let a malicious user execute arbitrary code; a format string vulnerability was reported when handling the 'ABLANG' environment variable, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in the 'setitem()' function when handling the 'PHOTON_PATH' environment variable due to a boundary error, which could let a malicious user execute arbitrary code; a vulnerability was reported in the 'phfont' utility due to a race condition, which could let a malicious user obtain root privileges; a buffer overflow vulnerability was reported in the 'su' utility due to a boundary error, which could let a malicious user execute arbitrary code; a Denial of Service vulnerability was reported when handling a certain command; a vulnerability was reported in the '/etc/rc.d/rc.local' file due to insecure file permissions, which could let a malicious user obtain root privileges; and a buffer overflow vulnerability was reported in the 'passwd' utility due to a boundary error, which could let a malicious user execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>An exploit script, DSR-QNX6.2.1-phfont.sh.txt, for the RTOS's phfont command vulnerability has been published.</p>	<p>QNX Neutrino RTOS</p> <p>Multiple Vulnerabilities</p> <p>CVE-2005-1528 CVE-2006-0618 CVE-2006-0619 CVE-2006-0620 CVE-2006-0621 CVE-2006-0622 CVE-2006-0623</p>	Not Available	<p>Secunia Advisory: SA18750, February 8, 2006</p>
<p>Softmaker Shop</p> <p>Softmaker Shop 0</p>	<p>Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required;</p>	<p>SoftMaker Shop</p> <p>Multiple Cross-Site Scripting</p> <p>CVE-2006-0532</p>	2.3	<p>Security Focus, Bugtraq ID: 16471, February 2, 2006</p>

	however, Proof of Concept exploits have been published.			
Sony Ericsson Mobile Communications AB Sony Ericsson K600i, T68i, V600i, W800i	A remote Denial of Service vulnerability has been reported in the L2CAP (Logical Link Control and Adaptation Layer Protocol) layer. No workaround or patch available at time of publishing. A Proof of Concept exploit script, bluetooth6.c, has been published.	Sony Ericsson Cell Phones Bluetooth L2CAP Denial of Service	Not available	Secunia Advisory: SA18747, February 8, 2006
SPIP SPIP 1.9.Alpha 1, 1.8.2-d	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'forum.php3' due to insufficient sanitization of the 'id_article' and 'id_forum' parameters being using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'index.php3' due to insufficient sanitization of the 'lang' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code. Updates available There is no exploit code required; however, an exploit script, spip_182g_shell_inj_xpl.html, has been published.	SPIP SQL Injection & Cross-Site Scripting CVE-2006-0518 CVE-2006-0519	2.3 (CVE-2006-0518) 2.3 (CVE-2006-0519)	Secunia Advisory: SA18676, February 1, 2006 Security Focus, Bugtraq ID: 16458, February 7, 2006 PacketStorm, February 9, 2006
Sun Microsystems, Inc. Java Web Start 1.x, Java JDK 1.5.x, Java JRE 1.5.x / 5.x	A vulnerability has been reported due to an unspecified error, which could let an untrusted application obtain elevated privileges. Updates available Currently we are not aware of any exploits for this vulnerability.	Java Web Start Sandbox Security Bypass CVE-2006-0613	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102170, February 7, 2006
Sun Microsystems, Inc. Sun JDK & JRE 5.0 Update 5 & prior, SDK & JRE 1.4.2_09 & prior, SDK & JRE 1.3.1_16 & prior	Seven vulnerabilities have been reported in Sun Java JRE (Java Runtime Environment) due to various unspecified errors in the 'reflection' APIs, which could let a remote malicious user compromise a user's system. Update information Currently we are not aware of any exploits for these vulnerabilities.	Sun Java JRE 'reflection' APIs Sandbox Security Bypass CVE-2006-0614 CVE-2006-0615 CVE-2006-0616 CVE-2006-0617	Not Available	Sun(sm) Alert Notification Sun Alert ID: 102171, February 7, 2006
Tachyondecay.net Vanilla Guestbook 1.0. Beta	Multiple input validation vulnerabilities have been reported which could let a remote malicious user execute arbitrary HTML, script code, and SQL code. No workaround or patch available at time of publishing. There is no exploit code required.	Tachyondecay Vanilla Guestbook Multiple Input Validation CVE-2006-0540 CVE-2006-0541	7 (CVE-2006-0540) 2.3 (CVE-2006-0541)	Security Focus, Bugtraq ID: 16464, February 1, 2006
Unknown Domain Shoutbox Unknown Domain Shoutbox 2005.7.21	Several vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of the 'Handle' and 'Message' fields, which could let a remote malicious user	Unknown Domain Shoutbox Cross-Site Scripting & SQL Injection	Not Available	Security Focus, Bugtraq ID: 16543, February 8, 2006

	<p>execute arbitrary HTML and script code; and SQL injection vulnerabilities were reported due to insufficient sanitization of various unspecified parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	CVE-2006-0605 CVE-2006-0606		
<p>vwdev</p> <p>vwdev</p>	<p>An SQL injection vulnerability has been reported due to insufficient validation of the 'UID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	vwdev SQL Injection	Not Available	Security Tracker Alert ID: 1015594, February 7, 2006

[\[back to top\]](#)

Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- [Sony Ericsson Cell Phones Bluetooth L2CAP Denial of Service](#): A remote Denial of Service vulnerability has been reported in the L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.
- [hcidump Bluetooth L2CAP Remote Denial of Service](#): A remote Denial of Service vulnerability has been reported in the L2CAP (Logical Link Control and Adaptation Layer Protocol) layer.
- [bss-0.6.tar.gz](#): A L2CAP layer fuzzer designed to assess the security of Bluetooth enabled devices by sending malicious packets.
- [Mobile email set to explode](#): According to a report from industry analysts, Datamonitor, mobile email is on the verge of mass adoption. There are roughly 650 million corporate email inboxes worldwide today and at least 35 per cent of which could be mobilized.

[\[back to top\]](#)

General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- [Cyber Storm Brewing For Homeland Security](#): The U.S. Department of Homeland Security is attempting to create a perfect storm in cyberspace. They are simulating a series of cyber attacks on critical infrastructure in the private sector and in international, federal and state governments in order to test response. The test is part of larger homeland defense plans and ordered by a presidential directive. It is designed to strengthen communications, coordination and partnerships. The threats are fictitious and take place in a contained, secure environment.
- [Exploit for QueryInterface Vulnerability in Mozilla](#): US-CERT is aware of publicly available exploit code for a memory corruption vulnerability in the Mozilla Firefox web browser and Thunderbird mail client.
- [XML Injection and Code Execution Vulnerabilities in Mozilla Suite](#): US-CERT is aware of several vulnerabilities in Mozilla. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary JavaScript commands with elevated privileges or cause a denial of service condition on a vulnerable system.
- [Spammed Trojan horse pretends to come from anti-virus company](#): According to experts at SophosLabs™, a Trojan horse has been spammed out to email addresses disguised as a message from a Finnish anti-virus company. The Troj/Stinx-U Trojan horse has been seen attached to email messages pretending to come from Helsinki-based F-Secure, and can have a subject line chosen from "Firefox Browsing Problem", "Mozilla Browsing Problem", or "Website Browsing Problem".
- [ID Theft And Internet Fraud Declining?](#) According to a report by Javelin Strategy and Research, incidents of fraud from Internet-based means may be on the decline. In cases where the source of the identity theft was known, only 9 percent were reported to have come from hacking, viruses and phishing. In contrast, a lost or stolen wallet or credit/debit card was the cause of 30 percent of the incidents. The study also found that fraudulent activity is mostly (over 70 percent) conducted offline via phone or mail.
- [Spyware Triples During 2005](#): According to anti-spyware developer Webroot, spyware tripled during 2005. At the start of the year Webroot identified only 40,000 traces and the year ended with 400,000 spyware-distributing sites and a global count of 120,000 different traces, or spyware components.

[\[back to top\]](#)

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folder.
2	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
3	Mytob-GH	Win32 Worm	Stable	November 2005	A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender's address.
4	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
5	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
6	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
7	Sober-Z	Win32 Worm	Stable	December 2005	This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security.
8	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
9	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.

10	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
----	--------	------------	--------	---------------	--

Table updated February 7, 2006

[\[back to top\]](#)

Last updated February 09, 2006